Search result: 1

(WO/2000/010303) ACCESS CONTROL USING ATTRIBUTES CONTAINED WITHIN PUBLIC KEY CERTIFICATES

Latest bibliographic data on file with the International Bureau

Publication Number: WO/2000/010303 **International Application No.:** PCT/IB1999/001452
Publication Date: 24.02.2000 **International Filing Date:** 30.07.1999
Chapter 2 Demand Filed: 08.03.2000

Int. Class.: ***H04L 12/22*** (2006.01), ***H04L 29/06*** (2006.01)

Applicant: **KYBERPASS CORPORATION** [CA/CA]; Suite 110 One Antares Drive Nepean, Ontario K2E 8C4 (

Inventor: **HAVERTY, Rand**; Kyberpass Corporation Suite 110 One Antares Drive Nepean, Ontario K2E 8C4

Agent: **SEAS, Robert, J.**; Sughrue, Mion, Zinn, Macpeak & Seas, PLLC Suite 800 2100 Pennsylvania Ave N.W. Washington, DC 20037-3202 (US).

Priority Data: 09/132,672 12.08.1998 US

Title: ACCESS CONTROL USING ATTRIBUTES CONTAINED WITHIN PUBLIC KEY CERTIFICATES

Abstract: In Public Key Infrastructure ('PKI') applications, a key pair (public key and private key) is used to provide strong authentication and encryption services. The key pair is associated with the user by the use of a 'certificate,' which contains the user's public key as well as attributes associated with that use This invention relates to the use of these attributes to control the access to a protected resource given to authenticated users. The attributes within a user's public key certificate are filtered by an attribute filter referenced by the proxy definition in order to control access to a protected resource. Further limitation of access to a protected resource is accomplished by association with server input and outp addresses.

Designated States: AU, CA, CN, JP, SG.
European Patent Office (EPO) (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT SE).

Publication Language: English (EN)

Filing Language: English (EN)

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－523816
（P2002－523816A）
(43)公表日　平成14年７月30日(2002.7.30)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ　５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ　５Ｊ１０４
			６７３Ａ

審査請求　未請求　予備審査請求　有　（全 35 頁）

(21)出願番号　特願2000－565651(P2000－565651)
(86)（22)出願日　平成11年７月30日(1999.7.30)
(85)翻訳文提出日　平成13年２月９日(2001.2.9)
(86)国際出願番号　ＰＣＴ／ＩＢ９９／０１４５２
(87)国際公開番号　ＷＯ００／１０３０３
(87)国際公開日　平成12年２月24日(2000.2.24)
(31)優先権主張番号　０９／１３２，６７２
(32)優先日　平成10年８月12日(1998.8.12)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＡＵ，ＣＡ，ＣＮ，ＪＰ，ＳＧ

(71)出願人　カイバーパス　コーポレーション
カナダ、オンタリオ　ケー２イー　８シー４、ネピアン、ワン　アンタレス　ドライブ　（番地なし）、スイート110
(72)発明者　ヘーバティー、ランド
カナダ、オンタリオ　ケー２イー　８シー４、ネピアン、ワン　アンタレス　ドライブ　（番地なし）、スイート110、カイバーパス　コーポレーション
(74)代理人　弁理士　北澤　一浩　（外２名）
Ｆターム(参考)　5B085 AE03 AE09
5J104 AA07 KA05 NA02 NA05 PA07

(54)【発明の名称】　公開鍵証明書に含まれたアトリビュートを使用するアクセス制御

(57)【要約】
公開鍵インフラストラクチャ（ＰＫＩ）の応用で、一対の鍵（公開鍵と非公開鍵）を使用して強力な認証と暗号化サービスを提供する。一対の鍵は、ユーザの公開鍵とユーザに関連させたアトリビュートを含む「証明書」の使用によりユーザと関連させる。本発明はそのアトリビュートを使用して、認証したユーザに保護リソースへのアクセスを制御する。ユーザ公開鍵証明書内のアトリビュートは保護リソースへのアクセスを制御するためにプロクシ定義により参照したアトリビュート・フィルタによってフィルタ処理される。保護リソースへのアクセスの別な制限はサーバ入力と出力アドレスに関連させておこなう。

【特許請求の範囲】

【請求項１】　クライアント・ステーションのユーザからコンピュータ・リソースへのアクセス要求のサーバ認証方法において、

上記サーバに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記サーバにアトリビュート・フィルタを記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算出値を上記サーバで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記サーバで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記サーバで判定するステップとを有することを特徴とするアクセス要求のサーバ認証方法。

【請求項２】　上記サーバにアトリビュート・フィルタを記憶させる上記ステップは、

上記アトリビュート・フィルタの識別を判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有することを特徴とする、請求項１に記載のアクセス要求のサーバ認証方法。

【請求項３】　上記演算するステップは、

上記証明書を検索するために上記サーバを探索するステップと、

上記証明書が上記サーバに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有することを特徴とする、請求項１に記載のアクセス要求のサーバ認証方法。

【請求項４】　上記演算するステップは、

上記証明書の中の使用可能なアトリビュートの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビ

ュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項１に記載のアクセス要求のサーバ認証方法。

【請求項５】 クライアント・ステーションのユーザからコンピュータ・リソースへのアクセス要求のサーバ認証の方法において、

上記サーバに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記サーバにアトリビュート・フィルタを記憶させるステップと、

上記サーバにプロクシ定義を記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから導いた算出値を上記サーバで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記サーバで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記サーバで判定するステップとを有することを特徴とするアクセス要求のサーバ認証方法。

【請求項６】 上記サーバにアトリビュート・フィルタを記憶させる上記ステップは、

上記証明書内の使用可能なアトリビュートを判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有することを特徴とする、請求項５に記載のアクセス要求のサーバ認証方法。

【請求項７】 上記サーバにプロクシ定義を記憶させるステップは、上記アトリビュート・フィルタを参照するプロクシ定義要素を付加するステップを含むことを特徴とする、請求項５に記載のアクセス要求のサーバ認証方法。

【請求項８】 上記ユーザと関連したアトリビュートを含む証明書を上記サーバに記憶させるステップは、

上記証明書を検索するために上記サーバを探索するステップと、

上記証明書が上記サーバに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有することを特徴とする、請求項５に記載のアクセス要求のサーバ認証方法。

【請求項９】　上記演算するステップは、

上記プロクシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項５に記載のアクセス要求のサーバ認証方法。

【請求項１０】　上記演算するステップは、

上記プロクシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記サーバの入力アドレスを使用して上記選択したアトリビュートを評価することにより、上記算出値を判定するステップとを有することを特徴とする、請求項５に記載のアクセス要求のサーバ認証方法。

【請求項１１】　上記演算するステップは、

上記プロクシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記保護コンピュータ・リソースの出力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項５に記載のアクセス要求

のサーバ認証方法。

【請求項１２】 クライアント・ステーションのユーザから、コンピュータ・リソースへのアクセス要求の認証に適したコンピュータ・システムにおいて、

プロセッサとメモリから成り、

上記コンピュータ・システムに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記コンピュータ・システムにアトリビュート・フィルタを記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算出値を上記コンピュータ・システムで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記コンピュータ・システムで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記コンピュータ・システムで判定するステップとを、

上記コンピュータ・システムが実行可能となるようにしたソフトウェア・インストラクションを上記メモリが含むことを特徴とするアクセス要求の認証に適したコンピュータ・システム。

【請求項１３】 上記メモリは、上記コンピュータ・システムが更に、

上記アトリビュート・フィルタの識別を判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザアトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを、

実行可能となるソフトウェア・インストラクションを有することを特徴とする、請求項１２に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項１４】 上記メモリは、上記コンピュータ・システムが更に、

上記証明書を検索するために上記コンピュータ・システムを探索するステップと、

上記証明書が上記コンピュータ・システムに見つからないなら遠隔の証明書保

存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを、

実行可能となるソフトウェア・インストラクションを有することを特徴とする、請求項１２に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項１５】 上記メモリは、上記コンピュータ・システムが更に、

上記証明書の中の使用可能なアトリビュートの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを、

実行可能となるソフトウェア・インストラクションを更に有することを特徴とする、請求項１２に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項１６】 クライアント・ステーションのユーザから、コンピュータ・リソースへのアクセス要求の認証に適したコンピュータ・システムにおいて、

プロセッサとメモリから成り、

上記コンピュータ・システムに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記コンピュータ・システムにアトリビュート・フィルタを記憶させるステップと、

上記コンピュータ・システムにプロクシ定義を記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算出値を上記コンピュータ・システムで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記コンピュータ・システムで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記コンピュータ・システムで判定するステップとを、

上記コンピュータ・システムが実行可能となるようにしたソフトウェア・インストラクションを上記メモリが含むことを特徴とするアクセス要求の認証に適し

たコンピュータ・システム。

【請求項１７】 上記証明書内で使用可能なアトリビュートを判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有するように、上記コンピュータ・システムでアトリビュート・フィルタを記憶させるステップを更に該コンピュータ・システムが実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項１６に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項１８】 上記アトリビュート・フィルタを参照するプロクシ定義要素を付加するステップを有するように、プロクシ定義を記憶させるステップを上記コンピュータ・システムが更に実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項１６に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項１９】 上記証明書を検索するために上記コンピュータ・システムを探索するステップと、

上記証明書が上記コンピュータ・システムに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有するように、上記コンピュータ・システムで上記ユーザと関連したアトリビュートを含む証明書を記憶させるステップを更に該コンピュータ・システムが実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項１６に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項２０】 上記証明書の中の使用可能なアトリビュートの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有するように、上記コンピュータ・システムが演算ステップを更に実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項１６に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項２１】　上記プロクシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記コンピュータ・システムの入力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップとを有するように、上記コンピュータ・システムが演算ステップを更に実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項１６に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項２２】　上記プロクシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記保護コンピュータ・リソースの出力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップを有するように、上記コンピュータ・システムが演算ステップを更に実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項１６に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項２３】　クライアント・ステーションのユーザから、コンピュータ・リソースへのアクセス要求の認証をコンピュータができるためのコンピュータ・プログラム製品において、

上記コンピュータが所定のオペレーションをおこなうことが可能なソフトウェ

ア・インストラクションと、該インストラクションを運ぶコンピュータ読み取り可能な媒体とを有し、

上記所定オペレーションは、

上記コンピュータに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記コンピュータにアトリビュート・フィルタを記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算出値を上記コンピュータで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記コンピュータで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記コンピュータで判定するステップとを含むことを特徴とするアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項２４】　上記コンピュータにアトリビュート・フィルタを記憶させる上記ステップは、

上記アトリビュート・フィルタの識別を判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有することを特徴とする、請求項２３に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項２５】　上記ユーザと関連したアトリビュートを含む証明書を上記サーバに記憶するステップは、

上記証明書を検索するために上記サーバを探索するステップと、

上記証明書が上記サーバに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有することを特徴とする、請求項２３に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項２６】　上記アトリビュート・フィルタを使用して上記証明書内の上記アトリビュートから算出値を上記サーバで演算するステップは、

上記証明書の中の使用可能なアトリビュートの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項２３に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項２７】　クライアント・ステーションのユーザから、コンピュータ・リソースへのアクセス要求の認証をコンピュータができるためのコンピュータ・プログラム製品において、

上記コンピュータが所定のオペレーションをおこなうことが可能なソフトウェア・インストラクションと、該インストラクションを運ぶコンピュータ読み取り可能な媒体とを有し、

上記所定オペレーションは、

上記コンピュータに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記コンピュータにアトリビュート・フィルタを記憶させるステップと、

上記コンピュータにプロクシ定義を記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算出値を上記コンピュータで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記コンピュータで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記コンピュータで判定するステップとを有することを特徴とする、アクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項２８】　上記コンピュータにアトリビュート・フィルタを記憶させる上記ステップは、

上記証明書内で使用可能なアトリビュートを判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有することを特徴とする、請求項２７に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項２９】　上記コンピュータにプロクシ定義を記憶させるステップは、上記アトリビュート・フィルタを参照するプロクシ定義要素を付加するステップを含むことを特徴とする、請求項２７に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項３０】　上記ユーザに関連したアトリビュートを含む証明書を上記コンピュータに記憶させるステップは、

上記証明書を検索するために上記コンピュータを探索するステップと、

上記証明書が上記コンピュータに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有することを特徴とする、請求項２７に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項３１】　上記アトリビュート・フィルタを使用して上記証明書内の上記アトリビュートから得た算出値を上記サーバで演算するステップは、

上記プロクシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項２７に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項３２】　上記アトリビュート・フィルタを使用して上記証明書内の上記アトリビュートから得た算出値を上記サーバで演算するステップは、

上記プロクシ定義により参照した上記アトリビュート・フィルタの検索ステッ

プと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記サーバの入力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップを有することを特徴とする、請求項２７に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項３３】　上記アトリビュート・フィルタを使用して上記証明書内の上記アトリビュートから得た算出値を上記サーバで演算するステップは、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記保護リソースの出力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項２７に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開鍵証明書とプロクシ定義内に含まれたユーザ・アトリビュートに基づいた、保護されたリソースへのアクセスを制御する方法に関する。また、本発明は公開鍵証明書とプロクシ定義内に含まれたユーザ・アトリビュートに基づいた、保護リソースへのアクセスを制御するソフトウェアを有するプログラム製品に関する。さらに、本発明は公開鍵証明書とプロクシ定義内に含まれたユーザ・アトリビュートに基づいた、保護リソースへのアクセスを制御するためのオペレーションをおこなうコンピュータ・システムに関する。

【０００２】

【従来の技術】

公開鍵インフラストラクチャ（パブリック・キー・インフラストラクチャ：ＰＫＩ）技術の出現前には、保護コンピュータ・リソースへの複数のユーザのアクセスを制御するために、トランザクション・プログラムの実行やデータベースをホスト化するなどの、いくつかの技術が発展した。保護方法の一つは物理的手段により保護対象のコンピュータ・システムへの認可されてないアクセスを防ぐことであった。この種の方法のうち最も簡単のものは、保護コンピュータ・システムにつながる端末へのアクセスを制限することであった。別の方法は、保護コンピュータ・システムと公共コンピュータ・ネットワーク間の物理的なネットワーク接続を許可しないことにより、認可してないアクセスを防ぐことであった。さらに別の保護方法は、保護コンピュータ・システムあるいは保護サーバの各々について自動的なアクセス制御システムを履行することであった。効果はあるが、これらの技術はコンピュータ・リソースの効果的な利用を抑制するという重大な欠点を抱えている。物理的なセキュリティ方法の場合には、インターネットのような公共ネットワークを保護コンピュータ・システムへのアクセスのために利用する機会が失われる。同様に、サーバ・レベルで履行される自動アクセス制御システムは特定のサーバにだけ適用可能である。つまり、アクセス制御の権利の管理はいくつかのサーバ間で重複することになり、間違いや混乱を発生し、また最

終的にコストの増大につながる。

【０００３】

インターネットおよび各種法人のイントラネットのような公共ネットワークの長所を生かすために、産業界はセキュリティ施策を実行するためのセキュリティ・サーバを利用する方法を採用している。セキュリティ・サーバは保護コンピュータ・リソースとクライアント・ステーション間に配置され、リソースとクライアント間の単独リンクとして働く。クライアントはセキュリティ・サーバに直接接続させることが可能であり、あるいは１個以上の通信ルータを介してセキュリティ・サーバにリンクさせることが考えられる。さらに、セキュリティ・サーバは単独のリソースまたは複数のリソースを保護することも可能である。ユーザが適切に認証される時のみ、このセキュリティ・サーバは保護リソースとクライアント・ステーション間の通信リンクを確立することになる。「セキュリティ・サーバ」という用語は、この意味において、セキュリティ・サーバ、ファイアウォール、プロクシ（代理）サーバ、認証サーバ等を含む。さらに、「保護リソース」という用語は保護対象のデータベース・サーバ、アプリケーション・サーバおよびトランザクション・サーバを含むが、これらに限定されない。

【０００４】

セキュリティ・サーバと組み合わせる方策は公開鍵インフラストラクチャ（ＰＫＩ）技術である。ＰＫＩの適用では、公開鍵と非公開鍵の一対の鍵（パブリック・キーとプライベート・キー）を使用して強力な認証と暗号化作業をおこなう。この一対の鍵はユーザについてのアトリビュートに加え、ユーザの公開鍵を含む「証明書」の使用によりユーザと関連づけられる。セキュリティ・サーバはプロクシを確立することによりクライアント・ステーション（あるいは通信ルータ）と保護リソース間のリンクを設立する。このプロクシは、クライアント・ステーションが適切に認証される場合にだけ作動させる。通常、このクライアント・ステーション認証は、クライアント・ステーションが公開鍵にアクセスするために正確なパスワードの提示、および実際の非公開鍵の入手に基礎をおいている。

【０００５】

【発明が解決しようとする課題】

本発明の目的は公開鍵証明書に記憶させたアトリビュートに基づいたセキュリティ・サーバにおいてアクセス制御機能を加える方法を提供する。公開鍵証明書に記憶させたどのアトリビュートもセキュリティ・サーバを介して保護リソースへのアクセスを制御するために使用できる。

【０００６】

【課題を解決するための手段】

本発明によれば、セキュリティ・サーバを介するアクセスを許可あるいは拒絶する新規な方法は、アトリビュートの値に基盤を置く。すなわち本発明の方法は、アトリビュートの値に基づいた条件をセキュリティ・サーバ内のプロクシと直接関連させるようにする。クライアント・ステーションと保護リソース間のプロクシはアクセス要求者が認証された時、および、そのプロクシに関連したアトリビュート条件が満たされる時のみ確立される。

【０００７】

本発明によれば、セキュリティ・サーバを介して保護リソースへのアクセスを制限する新規な方法はプロクシ定義と関連させた入出力アドレスに基づいたものである。すなわち本発明の方法は、アドレスに基づいた条件が特定のリソースにたいしてだけのアクセスを制限できるようにしたものである。

【０００８】

【発明の実施の形態】

本発明の望ましい実施の形態を、初めにイントラネットのような内部ネットワークから保護リソースにアクセスするクライアント・ステーションについて説明する。その後、インターネット、あるいは他の同様な公共ネットワークのような外部ネットワークから保護リソースにアクセスするクライアント・ステーションについて説明する。これら２種の望ましい実施の形態は、この２種の応用だけでなく、他の広範囲な環境に対しても適用可能である。つまり、この実施の形態は極めて一般的な意味で本発明を例示する役割を果たすことになる。

【０００９】

セキュリティ・サーバ方法

セキュリティ・サーバ方法は図１に簡潔に示してある。図中１００のクライア

ント・ステーションは、汎用あるいは特製コンピュータ・システムにて実行するプロセスと理解することができる。プロセスとしてのクライアント・ステーション１００は、保護リソース上のアプリケーションに関するタスクの実行を要求するユーザと考えることができる。

【００１０】

図１では、１０１がセキュリティ・サーバを示し、１０２は保護リソースを示す。図１から分かるように、クライアント・ステーション１００と保護リソース１０２間には直接の通信リンクは存在しない。セキュリティ・サーバ１０１は汎用あるいは特製コンピュータ・システムで走行するプロセスと考えられる。同様に、保護リソース１０２もプロセスと考えられる。

【００１１】

保護リソース１０２へのアクセスを望むユーザは、セキュリティ・サーバ１０１を介してユーザのクライアント・ステーション１００からアクセスしなくてはならない。保護リソース１０２へのアクセスが認可されたユーザはセキュリティ・サーバ１０１により認証を受け、保護リソース１０２を利用することを許可される。セキュリティ・サーバ１０１は認可を受けてないユーザの保護リソース１０２へのアクセスを防止する。

【００１２】

図２はより洗練されたコンピュータ・ネットワークを示し、おそらく現行の環境において一般的に見られるものである。クライアント・ステーション１００は保護リソース１０２へ到達可能な２つの経路を有する。

【００１３】

最短の経路はセキュリティ・サーバ１０１への通信ルータ１１２を経由する接続である。セキュリティ・サーバ１０１によりユーザが適切に認証を受けると、プロクシを経由して保護リソース１０２へのアクセスが許可される。通信ルータ１１２の唯一の役割はクライアント・ステーション１００とセキュリティ・サーバ１０１間の接続を容易にすることである。

【００１４】

別の経路は通信ルータ１１１を経由してファイアウォール１１３への接続を確

立するものである。ファイアウォール１１３は通信リンクをサポートし、セキュリティ・サーバ１０１と同じようにしてイントラネット１１４へのアクセスを提供する。これは関連のリソースが外部的にアクセスできるのに加え内部的にもアクセス可能となることを考えると、近代的な方法である。イントラネット１１４はセキュリティ・サーバ１０１に物理的に接続されている。ユーザがイントラネット１１４にアクセスすることが許可されたなら、セキュリティ・サーバ１０１は保護リソースへの認可されてない割り込みを妨げる。ユーザが本物であり適切に認証されるなら、プロクシを経由して保護リソース１０２へのアクセスが許可される。見て分かるように、図２は今日のコンピュータ環境で考えられる潜在的なネットワークの組み合わせ全てを示しているわけではない。理解を容易にするため、「クライアント・ステーション」という用語は、ユーザが現在アクセスしているコンピュータ・システムだけではなく、クライアント・ステーション１００とセキュリティ・サーバ１０１間にあるシステム全て（例えば、通信ルータ、ファイアウォール、イントラネット）を含むものとする。

【００１５】

クライアント・ステーション１００、セキュリティ・サーバ１０２、保護リソース１０３など全てが走行するコンピュータ・システムは、一般的には、かなりの距離を取って離した物理的に異なったコンピュータ・システムである。この配列は一つの典型例ではあるが、上記３つのプロセスが物理的に異なったコンピュータ・システム上を走行しない時、あるいは、かなり距離を取って離したコンピュータ・システムでない時でさえもこのセキュリティ・サーバ方式のコンセプトを適用する。しかし、この説明の一般的に意味するものは、ここに説明した典型的配列に関することである。

【００１６】

このコンピュータ・システムが通信する方法は高い水準で取り扱われ、その詳細は本発明を分かり易くするため省略する。この通信についての詳細な情報は、「データおよびコンピュータ・通信（Ｄａｔａ ａｎｄ Ｃｏｍｐｕｔｅｒ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）」あるいは「ローカル・ネットワーク（Ｌｏｃａｌ Ｎｅｔｗｏｒｋｓ）」を参照することで得られる。両文献は共にウィリアム

・ストーリングスによる著作であり、その全体は本出願の有用な背景情報の引用文献として示す。

【００１７】

実用レベルでのプロセス（クライアント・プロセス、セキュリティ・サーバ・プロセスおよびアプリケーション・サーバ・プロセスなどを含む）は様々な媒体の一つでソフトウェアとして供給される。さらに、実際のソフトウェアはプログラム言語あるいはプログラム言語で書かれた文書に基づくものである。こうしたプログラム言語文書はコンピュータにより実行した時に、その文書の特定の内容に基づいてコンピュータを作動させ、所定の方法で限定的なプロセスを走行させる。また、ソフトウェアは、オリジナルのソース・コード、アセンブリ・コード、オブジェクト・コード、機械言語、それらの圧縮化バージョンあるいは暗号化バージョン、などを含む。但し、これらに限定されない多数の形で提供することが考えられる。

【００１８】

コンピュータ・システムにおいて良く知られているものは「媒体」あるいは本願で使用する「コンピュータ読み取り可能媒体」であり、具体的にはフロッピー（登録商標）ディスク、磁気テープ、コンパクト・ディスク、集積回路、カートリッジ、通信回路を介する遠隔伝送、またはコンピュータで使用可能な他の同様な媒体である。例えば、プロセスを定義するソフトウェアを供給するためには、供給者はフロッピーディスクを提供するか、衛星通信や直接の電話回線やインターネットなどを介して、様々な形のソフトウェアを伝送することが考えられる。

【００１９】

こうしたソフトウェア・インストラクションはフロッピーディスクに「書き込まれる」か、集積回路に「記憶させる」か、通信回路で「運搬される」かであるが、ここでの説明の目的から考慮すると、コンピュータで使用可能な媒体はソフトウェアを「運ぶ」と称することにする。このように、「運ぶ」という用語はソフトウェアがコンピュータで使用可能な媒体に関連させる上記方法および同等の全ての方法を含むものである。

【００２０】

従って、説明を分かり易くするため、「プログラム製品」という用語は、これ以後、上記のようにソフトウェアを適切な方法で運ぶコンピュータで使用可能な媒体に関して使用する。

【００２１】

プロクシ

図１では、セキュリティ・サーバ１０１の入力アドレスはクライアント・ステーション１００とのインターフェースを有する。セキュリティ・サーバ１０１の出力アドレスは保護リソース１０２とのインターフェースを有する。セキュリティ・サーバ１０１にあるプロクシ定義は、セキュリティ・サーバ１０１の出力アドレスとセキュリティ・サーバ１０１の入力アドレス間の正確な対応を条件として指定する。プロクシ定義に含まれた情報は、どのように入力アドレスのトラフィックが指定された出力アドレスに経路を定められるかを決定する。さらに、プロクシ定義に含まれたこの情報が、プロクシ定義に含まれる全ての要素が考慮されることを確実にする。

【００２２】

プロクシ定義は、以下に示すようなプライバシー、セキュリティ、およびアクセス制御に関する多くの要素を有する。

１．記号プロクシ名。

２．ＦＴＰやＨＴＴＰのような関連したプロトコル。

３．接続に含むべき、あるいは除外すべきアドレスを特定する入力アドレス（例えば、ＴＣＰ／ＩＰ）フィルタ。

４．クライアントとサーバ間の全てのユーザおよび／あるいはデータのトラフィックを示す認証。

５．クライアントとサーバ間の全トラフィックを出所で暗号化し、送り先で解読することを示す暗号化。

６．クライアントとサーバ間の全トラフィックを出所で圧縮し、送り先で復帰（圧縮解除）することを示す圧縮。

７．入力アドレス（セキュリティ・サーバのクライアント・ステーション側のアドレス）。

８．出力アドレス（保護リソースに接続したセキュリティ・サーバの「保護」側のアドレス）

９．保護リソース・アドレス（どのプロクシに対してもいくつかある）。

【００２３】

証明書

表１はＸ．５０９バージョン３の公開鍵証明書の構成を示している。

【００２４】

【表１】

表　１　（Ｘ．５０９証明書）

証明書バージョン番号
証明書シリアル番号
証明書発行者の識別名アトリビュート
有効日付／時間以前不可／以後不可
被証明者の識別名アトリビュート
被証明者の公開鍵ビット
追加アトリビュート
発行者のデジタル署名ビット

【００２５】

アトリビュートのタイプ、証明書発行者と被証明者（証明書所有者）識別名を含む数値申し立て、有効日付、追加アトリビュートなどは、経路パスを制御したり、あるいは分離セキュリティ施策ドメイン用の規則を定義するためにセキュリティ・サーバによって使用可能である。例えば、ある仮想の会社がそれぞれ保護サーバを有する３つの、管理、製造、エンジニアリング部門があるとする。その保護サーバへのアクセスはセキュリティ・サーバを介する。管理部門のスタッフは自己の業務を達成するために管理サーバと製造サーバへのみアクセス可能である。エンジニアリング部門のスタッフは製造サーバとエンジニアリング・サーバへのアクセスが可能である。製造部門のスタッフは製造サーバへのアクセスのみ可能である。

【００２６】

標準的なＸ．５０９「組織ユニット名」アトリビュートは、従業員が当会社内のどこで働くかを示すために使用可能である。例えば、エンジニアリング部門で働くジョン・ドウは、一般名＝ジョン・ドウ、組織ユニット名＝エンジニアリング、組織名＝ハイポ・コーポレーション（仮想会社）等の識別名を有する。経理課で働いているジェーン・ドウは、一般名＝ジェーン・ドウ、組織ユニット名＝管理、組織名＝ハイポ・コーポレーション（仮想会社）等の識別名を有する。

【００２７】

この仮想会社では、セキュリティ・サーバは別々に各保護サーバに接続させてある。セキュリティ・サーバは、その発生点に拘わらず、従業員からの全ての接続要求を認証する。この従業員の組織ユニット名アトリビュート値がユーザのアクセス許可を判定するためにセキュリティ・サーバによって使われる。例えば、「エンジニアリング」の組織ユニット・アトリビュート値を持っている従業員だけがエンジニアリング・サーバへの接続を許可される。

【００２８】

証明書とアトリビュートの説明は「安全な電子商取引（Ｓｅｃｕｒｅ　Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｍｍｅｒｃｅ）」、Ｗ．フォード（Ｆｏｒｄ）とＭ．Ｓ．ボーム（Ｂａｕｍ）著、に見られる。証明書に含まれたアトリビュートは、一般名、地方名、州名あるいは郡名、組織名、組織ユニット名、国名、および街路住所などである（これに限定されない）。

【００２９】

認証手続き

図４はＰＫＩシステムに使用した、高レベル・ステップに変えた認証手続きを示す。これは一般化した手続きであり、認証手続きにおけるアトリビュート・フィルタを使用することをユーザに示すため用いる。

【００３０】

初めのステップ２００では、クライアント・ステーション１００がセキュリティ・サーバ１０１の公然のものとなったプロクシ・アドレスへの接続を求める。通信ルータ１１１と１１２、ファイアウォール１１３、イントラネット１１４は分かり易くするため図４から除外してある。前述のように、セキュリティ・サー

バ１０１へのアクセス要求はさまざまな経路をたどることができる。

【００３１】

ステップ２０１では、セキュリティ・サーバ１０１はクライアント・ステーション１００からの接続要求を受け入れる。接続要求の受け入れ後、ステップ２０２ではセキュリティ・サーバはクライアント・ステーション１００にログイン識別とパスワードを求める。

【００３２】

ステップ２０３では、セキュリティ・サーバ１０１からのログイン識別要求の受領により、クライアント・ステーション１００はユーザが非公開鍵の適切な保有者かどうか判定を求められる。クライアント・ステーション１００はユーザが非公開鍵を所有しており、しかも、ユーザがその鍵を適切に使用する必要な知識を有することを検証しなくてはならない。ユーザが適切に非公開鍵を使用できるなら、クライアント・ステーション１００はセキュリティ・サーバ１０１にユーザが非公開鍵を持っており、その鍵を適切に使用する知識があることを伝える。

【００３３】

ステップ２０４では、セキュリティ・サーバ１０１がユーザの公開鍵証明書に対してユーザのログオン情報を認証する。公開鍵証明書はセキュリティ・サーバ１０１あるいは遠隔の証明書保存場所に記憶させてある。公開鍵証明書が遠隔の保存場所に記憶させてあるなら、セキュリティ・サーバ１０１は認証手続きに入る前に公開鍵証明書を検索する。

【００３４】

ステップ２０５では、セキュリティ・サーバ１０１はユーザを検証すべきかどうか判定をおこなう。ステップ２０６では、ユーザが検証されたなら、保護リソースへのアクセスが許可される。それ以外は、ステップ２０７で、認証エラーのためにユーザが検証されないのでクライアント・ステーション１００からの接続が無効となる。

【００３５】

アトリビュート・フィルタ

本発明では、アトリビュート・フィルタとして知られている別の要素をブロク

シ定義に加える。このアトリビュート・フィルタの目的はユーザの公開鍵証明書にある特定のアトリビュート値に基づきセキュリティ・サーバ１００を介してアクセスを制御することである。セキュリティ・サーバ１００により使用されるプロクシ定義は、その一つがアトリビュート・フィルタ定義である一組の上記要素群から成る。アトリビュート・フィルタ定義はフィルタ名と「アクセス演算式」から成る。アトリビュート・フィルタ名はプロクシ定義にハード・コード化することが可能であるが、柔軟性は犠牲になる。アクセス演算式はブール演算式である（この演算式を書くための表記法の一つはインターネットＲＦＣ１９６０で定義したような「逆ポーランド表記法」であり、他の表記法も可能である。）

【００３６】

セキュリティ・サーバ１０１を介する保護リソース１０２へのアクセスは、アクセス演算式のブール演算式が接続要求時に本物と評価する時に認可される。アトリビュート・フィルタ用の簡単なブール演算式の一例は「ＣＮ＝Ｋｅｌｌｙ（ケリー）」である。この例では、接続を確立することを試みる要求者の一般名（ＣＮ）が「ケリー」であるなら、保護リソース１０２へのアクセスは許可されることになる。アトリビュート・フィルタ演算のアクセス演算式の演算は本物評価に限定されない、すなわち、保護リソース１０２へのアクセスはアクセス演算式が本物と評価したなら拒絶される可能性がある。

【００３７】

図５は、セキュリティ・サーバ１０１が公開鍵証明書に含まれるアトリビュートを評価する演算を実行する高水準ステップを示している。ステップ３０１では、セキュリティ・サーバ１０１がログオン要求（図４のステップ２０４を参照）を認証するため始動すると、記憶部から公開鍵証明書を検索する。ステップ３０２では、セキュリティ・サーバ１０１は公開鍵証明書が局地的に保存されているか、遠隔地に保存されているか判定する。遠隔地ならば、ステップ３０３は遠隔地記憶部から証明書を検索する。

【００３８】

ステップ３０４では、公開鍵証明書が検索されると、セキュリティ・サーバ１０１はクライアント・ステーション１００が要求したプロクシ定義を評価する。

セキュリティ・サーバ１０１は要求にあった特定の入力／出力アドレス指定に使用するプロクシ定義によって、どのアトリビュート・フィルタが求められているか判定しなくてはならない。前述のように、プロクシ定義は特定のプロクシ定義に適したアトリビュート・フィルタに対するポインタを含む。

【００３９】

ステップ３０５では、プロクシ定義により特定されたアトリビュート・フィルタを判定した後、セキュリティ・サーバ１０１はアトリビュート・フィルタ内のアクセス演算式を使用してアトリビュート・フィルタ内に並べられた特定の公開鍵証明書を評価する。アクセス演算式は様々な表記法で書かれる。インターネットＲＦＣ１９６０表記法だけの使用に限定されない。

【００４０】

ステップ３０６では、アクセス演算式が本物と評価したなら、次にステップ３０８では、セキュリティ・サーバ１０１は保護リソース１０２へのアクセスを許可する。それ以外、アクセス演算式が偽物と評価したら、ステップ３０７でセキュリティ・サーバ１０１は保護リソース１０２へのアクセスを拒絶する。前記のように、アクセスはアトリビュート・フィルタの初期セットアップに基づき、ステップ３０６が本物と評価する時にも拒絶される可能性がある。

【００４１】

入力／出力アドレス

アトリビュート・フィルタを使用する別の実施の形態は、プロクシ定義の入力アドレス要素あるいは出力アドレス要素と関連させてある。この組み合わせは保護リソースへのアクセスに対し、さらに制限するために使用できる。アトリビュート・フィルタが入力アドレス（セキュリティ・サーバ１０１のクライアント側）と組み合わせられ、しかもアクセス演算式が本物と評価したなら、セキュリティ・サーバを介する保護リソース１０２へのアクセスは出力アドレス（セキュリティ・サーバ１０１の保護側）で許可される、あるいは拒絶されることになる。アトリビュート・フィルタと出力アドレスを組み合わせることは保護リソース１０２へのアクセスを抑制する。アクセス演算式が本物と評価したなら、プロクシの出力側で特定の保護サーバ・アドレスでの保護リソース１０２へのセキュリテ

ィ・サーバ１０１を介するアクセスは許可される、あるいは拒絶されることになる。

【００４２】

図６はこのアクセス制御を履行するため必要な高水準ステップである。ステップ４０１では、公開鍵証明書が検索された後、セキュリティ・サーバ１０１は特定の入力／出力アドレス指定を目標にしたプロクシ定義により、どのアトリビュート・フィルタが求められるか判定する。

【００４３】

ステップ４０２では、セキュリティ・サーバ１０１はアトリビュート・フィルタが入力アドレスと関連があるか判定する。ステップ４０３で、セキュリティ・サーバ１０１が入力アドレスとの組み合わせを見つけたなら、このアトリビュート・フィルタは公開鍵証明書アトリビュートの評価を求めるアクセス演算式を持っているか判定するために再検討される。ステップ４０４では、アクセス演算式が評価される。ステップ４０６では、アクセス演算式が本物と評価したのでセキュリティ・サーバ１０１はどの保護リソース１０２へのアクセスも許可する。それ以外は、ステップ４０５で、アクセス演算式が偽物と評価したのでセキュリティ・サーバ１０１はアクセスを拒絶する。セキュリティ・サーバ１０１は接続要求を終了する。

【００４４】

ステップ４０７では、アトリビュート・フィルタが出力アドレスとの関連があるとセキュリティ・サーバ１０１が判定したなら、同様のプロセスが続く。しかし、アクセスはその出力アドレスで特定の保護リソース１０２へだけ許可される。

【００４５】

ステップ４１２では、アトリビュート・フィルタが入力アドレスか出力アドレスのどちらかと関連があるなら、アトリビュート・フィルタのプロセス処理は前述のように進行する。

【００４６】

他の実施の形態への一般化

本発明は実行すべきステップ群やプロトコルに関して説明してきたが、本発明は上記説明のステップによりオペレーションをおこなうコンピュータ・システム、および上記説明のステップによりコンピュータ・システムがオペレーションをおこなうことが可能なソフトウェアを運搬するプログラム製品に属するものである。

【００４７】

図では、ステップの順番は必ずしも厳密ではなく、あるステップは他のステップと並行、あるいは異なった順番でおこなうことが考えられる。

【００４８】

特定の実施の形態を詳細に説明したが、本発明はそうした実施例に限定されるものではなく、添付の特許請求の範囲に基づき、公開鍵証明書アトリビュートが長所を引き立たせるように使用可能である。

【００４９】

参照

１．安全な電子商取引（Ｓｅｃｕｒｅ Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｍｍｅｒｃｅ）、Ｗ．フォード（Ｆｏｒｄ）とＭ．Ｓ．ボーム（Ｂａｕｍ）、プレンタス・ホール（Ｐｒｅｎｔｉｃｅ Ｈａｌｌ） ＰＴＲ、１９９７。

２．インターネット ＲＦＣ１９６０、「ＬＤＡＰ検索フィルタのストリング表示（Ａ Ｓｔｒｉｎｇ Ｒｅｐｒｅｓｅｎｔａｔｉｏｎ ｏｆ ＬＤＡＰ Ｓｅａｒｃｈ Ｆｉｌｔｅｒｓ）」。

【図面の簡単な説明】

【図１】

保護リソースへのクライアント・ステーションからのアクセスを制限するためセキュリティ・サーバを使用する通常のコンピュータ・ネットワークを示す概略ブロック図。

【図２】

大人数ユーザ・システムに一般的に見られる特徴を組み込む、より洗練されたコンピュータ・システム・ネットワークを示す概略ブロック図。

【図３】

ユーザと、その特定のユーザで識別された公開鍵証明書との相関関係を説明する表。

【図４】

セキュリティ・サーバとクライアント・ステーション間の公開鍵と非公開鍵を用いた通常のユーザ・ログインおよび認証シーケンスを示す図。

【図５】

保護リソースへのアクセスを制御するため公開鍵証明書内のアトリビュートの使用を説明するフローチャート。

【図６】

保護リソースへのアクセスを制御するためプロクシ定義の入出力アトリビュートの使用を説明するフローチャート。

【符号の説明】

１００　クライアント・ステーション

１０１　セキュリティ・サーバ

１０２　保護リソース

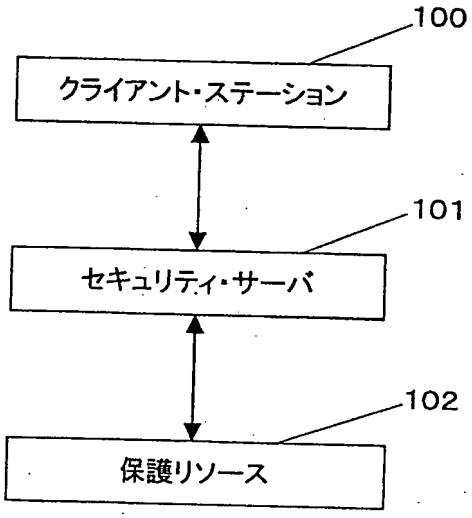
１１１　通信ルータ

１１２　通信ルータ

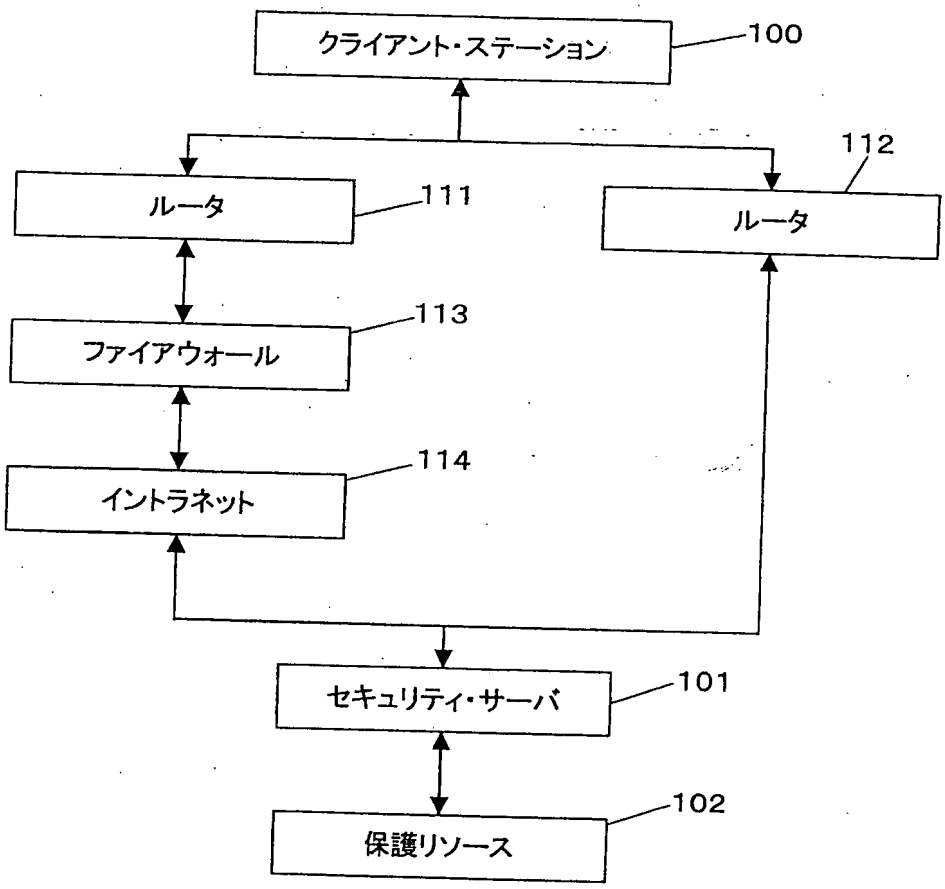
１１３　ファイアウォール

１１４　イントラネット

【図１】


100
クライアント・ステーション
101
セキュリティ・サーバ
102
保護リソース

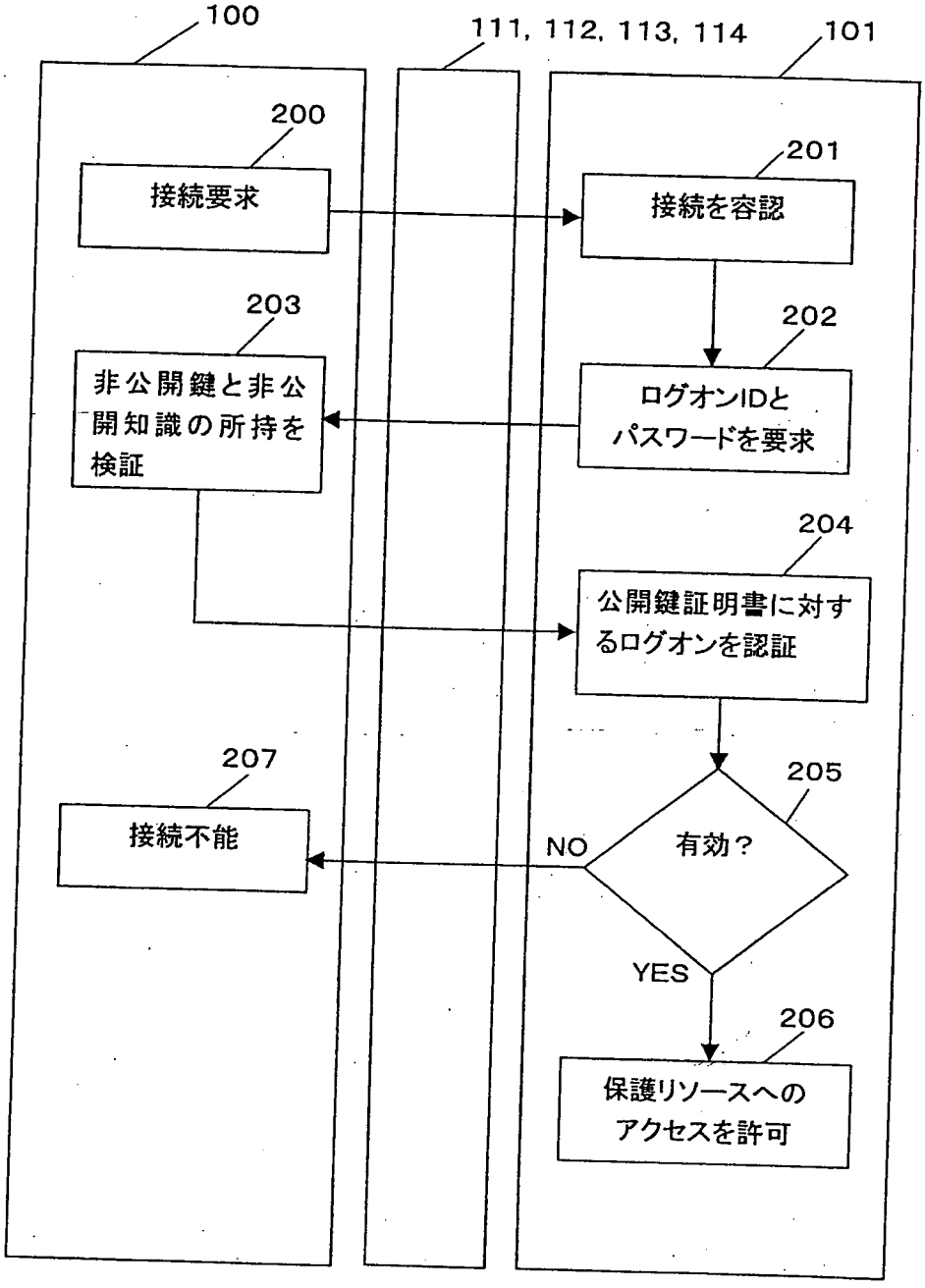
【図２】


クライアント・ステーション
100
112
ルータ
111
ルータ
113
ファイアウォール
114
イントラネット
セキュリティ・サーバ
101
保護リソース
102

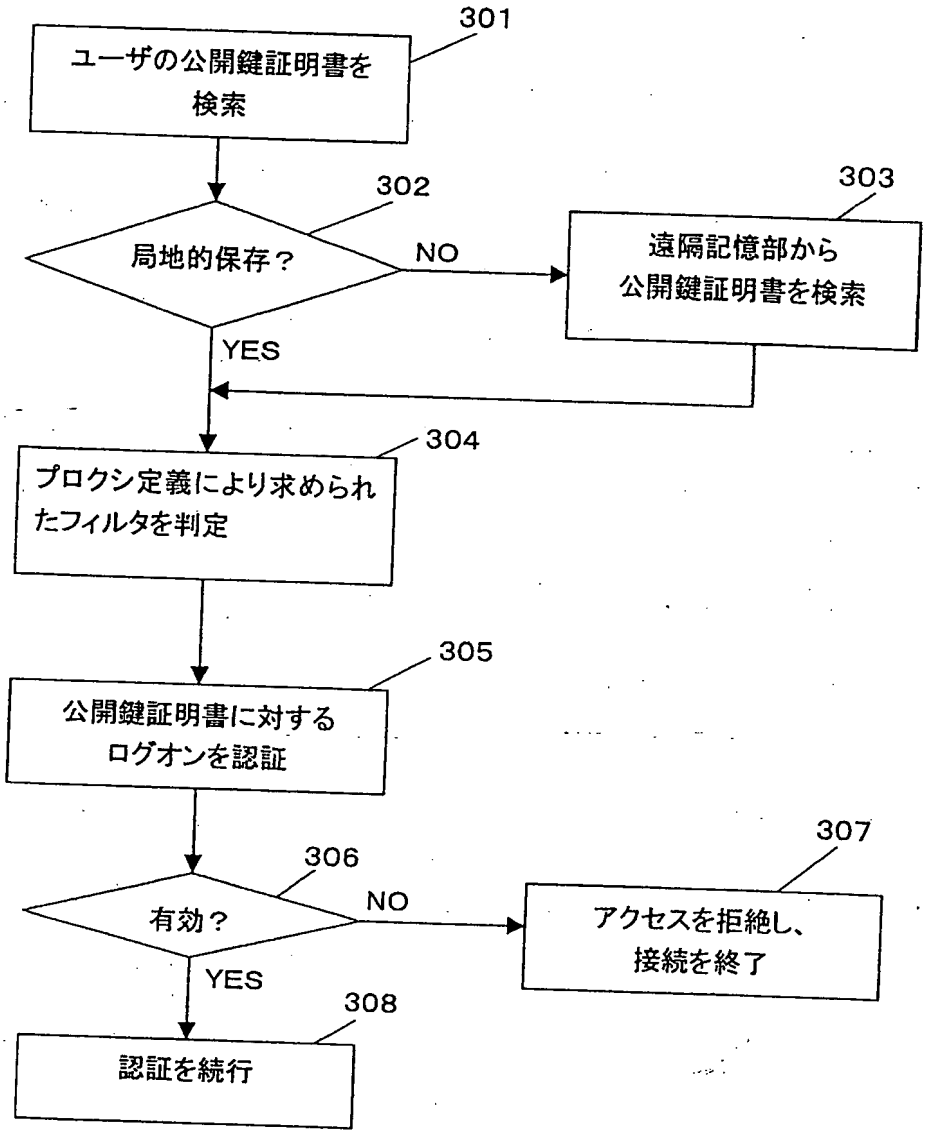
【図３】

証明書番号	ユーザ 名	公 開 鍵
1	ユーザ－１	公開鍵－１
2	ユーザ－２	公開鍵－２
3	ユーザ－３	公開鍵－３
4	ユーザ－４	公開鍵－４
n	ユーザ－ｎ	公開鍵－ｎ

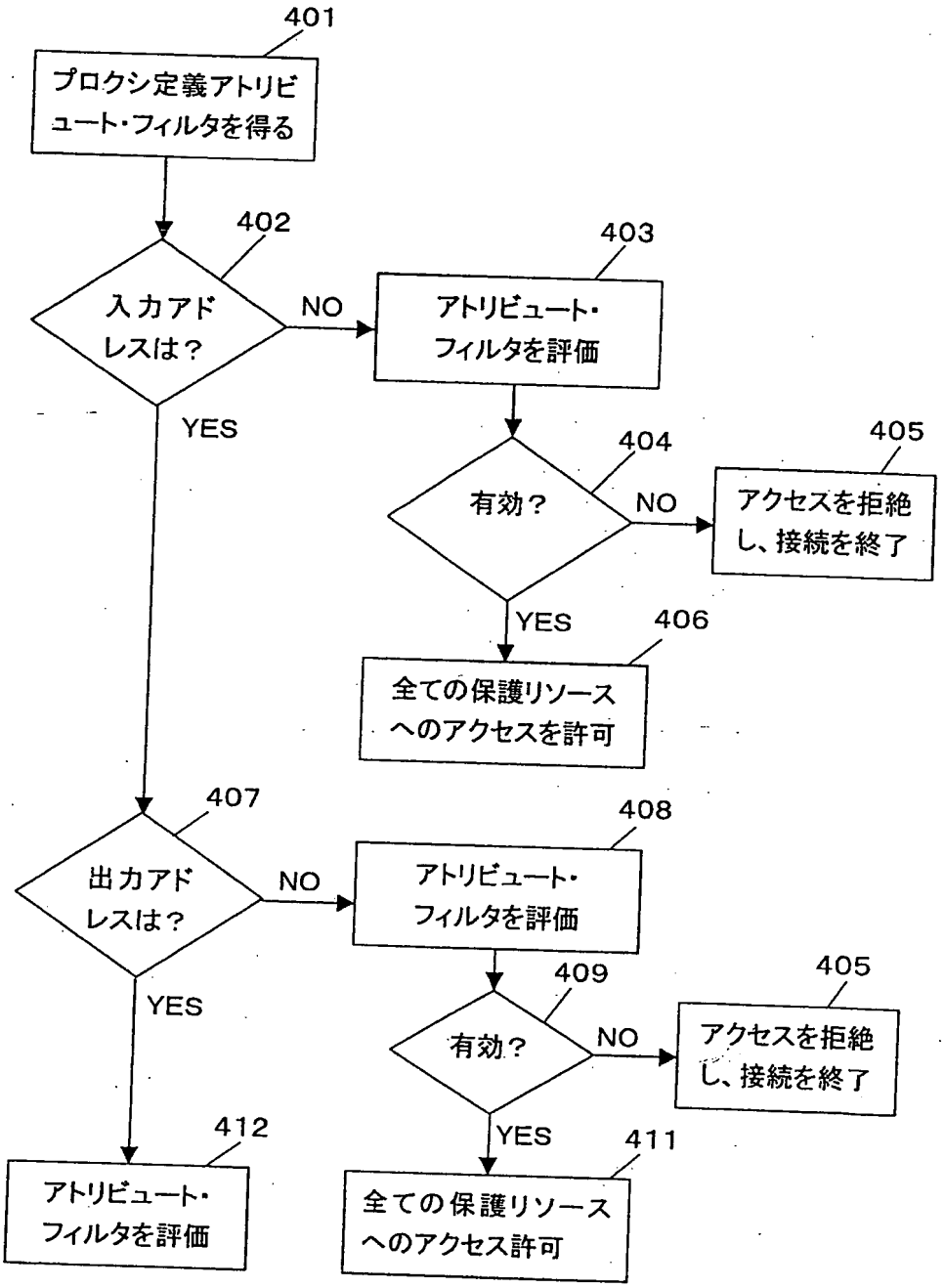
【図４】


100
111, 112, 113, 114
101
200
接続要求
201
接続を容認
203
非公開鍵と非公開知識の所持を検証
202
ログオンIDとパスワードを要求
204
公開鍵証明書に対するログオンを認証
207
接続不能
205
NO
有効？
YES
206
保護リソースへのアクセスを許可

【図５】


301
ユーザの公開鍵証明書を検索
302
局地的保存？
NO
303
遠隔記憶部から公開鍵証明書を検索
YES
304
プロクシ定義により求められたフィルタを判定
305
公開鍵証明書に対するログオンを認証
306
有効？
NO
307
アクセスを拒絶し、接続を終了
YES
308
認証を続行

【図６】


401
プロクシ定義アトリビュート・フィルタを得る
402
入力アドレスは？
NO
403
アトリビュート・フィルタを評価
YES
404
有効？
NO
405
アクセスを拒絶し、接続を終了
YES
406
全ての保護リソースへのアクセスを許可
407
出力アドレスは？
NO
408
アトリビュート・フィルタを評価
YES
409
有効？
NO
405
アクセスを拒絶し、接続を終了
YES
411
全ての保護リソースへのアクセス許可
412
アトリビュート・フィルタを評価

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/IB 99/01452

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PAYS P ET AL: "An intermediation and payment system technology" COMPUTER NETWORKS AND ISDN SYSTEMS,NL,NORTH HOLLAND PUBLISHING. AMSTERDAM, vol. 28, no. II, page 1197-1206 XP004018220 ISSN: 0169-7552 page 1199, right-hand column, line 19 -page 1201, left-hand column, line 24 page 1202, right-hand column, line 15 -page 1204, left-hand column, line 13 —— -/—	1-33

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family.

Date of the actual completion of the international search	Date of mailing of the international search report
17 December 1999	12/01/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer Lázaro López, M.L.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intl Jonal Application No
PCT/IB 99/01452

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 23062 A (NETIX INC T) 28 May 1998 (1998-05-28) page 7, line 28 -page 8, line 15 page 10, line 22 -page 12, line 19 page 13, line 20 -page 14, line 3 page 19, line 18 -page 20, line 9 page 21, line 17 -page 22, line 2 page 23, line 6-19 page 25, line 3 -page 29, line 4 page 31, line 8 -page 32, line 8	1-33
A	ANDERSON S ET AL: "Sessioneer: flexible session level authentication with off the shelf servers and clients" COMPUTER NETWORKS AND ISDN SYSTEMS,NL,NORTH HOLLAND PUBLISHING. AMSTERDAM, vol. 27, no. 6, page 1047-1053 XP004013206 ISSN: 0169-7552 page 1048, left-hand column, line 8 -page 1049, right-hand column, line 28 page 1050, left-hand column, line 32 -right-hand column, line 24	1-33
A	US 5 586 260 A (HU WEI-MING) 17 December 1996 (1996-12-17) column 1, line 47 -column 2, line 49 column 3, line 46 -column 5, line 3 column 5, line 65 -column 6, line 33	1-33
A	GARFINKEL S.: "Web Security & Commerce" June 1997 (1997-06) , O'REILLY , USA XP002126084 page 151, line 5 -page 156, line 16	1-33

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Int ional Application No
PCT/IB 99/01452

Patent document cited in search repor	Publication date	Patent family member(s)	Publication date
WO 9823062 A	28-05-1998	AU 7304798 A	10-06-1998
		EP 0938793 A	01-09-1999
US 5586260 A	17-12-1996	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)